INDEX BY AUTHOR

CRYPTOLOGIA

VOLUME 24 (2000)

Takahiro Abe and Hideki Sawada
34 Groups and RSA Cryptosystems
Russell Atkinson
361 David Brian Kern: Theft of Trade Secrets
Stephen Budiansky
119 Closing the Book on Pearl Harbor
Colin Burke
351 Letter to the Editor
Donald W. Davies
131 An Unidentified Cipher Device
Ralph Erskine
97 What Did the Sinkov Mission Receive from Bletchley Park?
Tzonelih Hwang and Chih-Hung Wang
148 (t,m) Threshold and Generalized ID-Based Conference Key Distribution System
David H. Hamer
41 G-312: An Abwehr Enigma
Thomas R. Hammant
235 Some Communications Intelligence in Tsarist Russia
333 The Magdeburg Incident: The Russian View
Stephen Huffman
289 The Navajo Code Talkers: A Cryptologic and Linguistic Perspective
Tzonelih Hwang, Narn-Yih Lee, Jiun-Jang Tsai, and Chuan-Ming Li
250 (t,n) Threshold-Multisignature Scheme and Generalized-MultiSignature Scheme Where Suspected Forgery Implies Traceability of Adversarial Shareholders
Philip H. Jacobsen
110 A Cryptologic Veteran's analysis of "Day of Deceit" - A Book Review
Lars R. Knudsen and Vincent Rijmen
135 Ciphertext-Only Attack on Akelarre
Louis Kruh
67 Reviews and Things Cryptologic
168 Reviews and Things Cryptologic
269 Reviews and Things Cryptologic
370 Reviews and Things Cryptologic

Narn-Yih Lee, Jiun-Jang Tsai, Chuan-Ming Li, and Tzonelih Hwang
250 (t,n) Threshold-Multisignature Scheme and Generalized-MultiSignature Scheme Where Suspected Forgery Implies Traceability of Adversarial Shareholders
Chuan-Ming Li, Tzonelih Hwang, Narn-Yih Lee, and Jiun-Jang Tsai
250 (t,n) Threshold-Multisignature Scheme and Generalized-MultiSignature Scheme Where Suspected Forgery Implies Traceability of Adversarial Shareholders
Philip Marks and Frode Weierud
55 Recovering the Wiring of Enigma's Umkehrwalze A
Craig McKay
321 From the Archives: Japanese Fears and the Ironies of Interception
Frederick D. Parker
212 How OP-20-G Got Rid of Joe Rochefort
Peter Pesic
193 The Clue to the Labyrinth: Francis Bacon and the Decryption of Nature
Cecil Phillips
324 The American Solution of a German One-Time-Pad Cryptographic System
Rebecca A. Ratcliff
160 Cryptology Through the Centuries: NSA's 1999 History Symposium
Vincent Rijmen and Lars R. Knudsen
135 Ciphertext-Only Attack on Akelarre
Shahrokh Saeednia
353 How to Make the Hill Cipher Secure
Hideki Sawada and Takahiro Abe
34 Groups and RSA Cryptosystems
John R. Schindler
339 A Hopeless Struggle: Austro-Hungarian Cryptology During World War I
Bruce Schneier
18 A Self-Study Course in Block-Cipher Cryptanalysis
Jiun-Jang Tsai, Chuan-Ming Li, Tzonelih Hwang, and Narn-Yih Lee
250 (t,n) Threshold-Multisignature Scheme and Generalized-MultiSignature Scheme Where Suspected Forgery Implies Traceability of Adversarial Shareholders
Chih-Hung Wang and Tzonelih Hwang
148 (t,m) Threshold and Generalized ID-Based Conference Key Distribution System
Frode Weierud and Philip Marks
55 Recovering the Wiring of Enigma's Umkehrwalze A
Heidi Williams
4 Applying Statistical Language Recognition Techniques in the Ciphertext-Only Cryptanalysis of Enigma

1 Annual Greg Mellen Memorial Cryptology Scholarship Prize
381 Index by Authors - Volume 24 (2000)